REMARKS

I. STATUS OF CLAIMS

Claims 1-36 are pending in the Application. Claims 3, 15, and 27 have been reinstated due to an error in the April 20, 2004, Advisory Action. Claims 1, 5, 6, 13, 17, 18, 25, 29, and 30 have been amended. It should be noted that Applicant has elected to amend said Claims solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent Business Goals, 65 Fed. Reg. 54603 (9/8/00). In making this amendment, Applicant has not and does not in any way narrow the scope of protection to which Applicant considers the invention herein to be entitled and does not concede, in any way, that the subject matter of such Claims was in fact taught or disclosed by the cited prior art. Rather, Applicant reserves Applicant's right to pursue such protection at a later point in time and merely seeks to pursue protection for the subject matter presented in this submission.

II. REJECTION BASED ON 35 U.S.C. §102(e)

The Office Action has rejected Claims 1-2, 4-14, 16-26, and 28-36 under 35 U.S.C. 102(e) as being anticipated by McManis (U.S. Pat. No. 5,757,914).

In a proper rejection under § 102(e) the cited reference must show each and every claimed feature in the same combination as arranged in the claim. See Lewmar Marine, Inc. v. Barient, Inc., 827 F.2d 744, 747-48, 3 USPQ2d 1766, 1768 (Fed. Cir. 1987). If even a single element or limitation is missing from the reference, anticipation is not found. Connell v. Sears, Roebuck & Co., 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983).

Applicant notes that Claims 3, 15, and 27 have been reinstated due to an error in the April 20, 2004, Advisory Action.

Claims 1, 13, and 25 have been amended to clarify the invention and appear as follows:

1. A method of securely invoking an access control function, the method comprising the steps of:

receiving a digital signature for the access control function;

generating a mapping of the access control function to the digital signature;

determining that the digital signature is mapped to the access control function based on the mapping when execution of the access control function is requested;

generating a digital signature for a retrieved executable element;

determining whether the executable element matches the access control function by comparing the digital signature of the executable element and the digital signature for the access control function;

executing the executable element only when the executable element matches the access control function;

wherein a particular class defines an implementation of the access control function; and

returning data to a caller of the executable element after executing the executable element.

13. A computer-readable medium carrying one or more sequences of one or more instructions for securely invoking an access control function, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving a digital signature for the access control function;

generating a mapping of the access control function to the digital signature;

determining that the digital signature is mapped to the access control function based on the mapping when execution of the access control function is requested;

generating a digital signature for a retrieved executable element;

determining whether the executable element matches the access control function by comparing the digital signature of the executable element and the digital signature for the access control function;

executing the executable element only when the executable element matches the access control function; and

wherein a particular class defines an implementation of the access control function; and

returning data to a caller of the executable element after executing the executable element.

25. An access control system, comprising:

a processor;

a memory coupled to the processor;

a first mapping that maps each of a set of access control functions to a digital signature of that access control function;

the processor configured to retrieve an executable element in response to a request to execute a first access control function;

the processor configured to generate a digital signature for a retrieved executable element;

the processor configured to determine whether the executable element matches the access control function by comparing the digital signature of the executable element and the digital signature for the access control function;

the processor configured to determine whether the executable element matches the first access control function based on the digital signature;

the processor configured to execute the executable element when the executable element matches the first access control function; and

wherein the set of access control functions are each implemented in a class; and

the processor configured to return data to a caller of the executable element after executing the executable element.

In particular, McManis does not teach or disclose a system that generates a digital signature for a retrieved executable element and determines whether the executable element matches the access control function by comparing the digital signature of the executable element and the digital signature for the access control function as claimed in Claims 1, 13, and 25. McManis does not contemplate such a system. McManis teaches away from such a system by teaching that a digital signature must be decoded and the decoded digital signature is compared to a generated message digest (col. 2, lines 22-36).

Further, McManis does no teach or disclose a system that returns data to a caller of the executable element after executing the executable element as claimed in Claims 1, 13, and 25. McManis does not mention such a feature and therefore does not contemplate such a system.

McManis therefore does not teach every aspect of the claimed invention.

Claims 1, 13, and 25 are therefore allowable.

Claims 2-12, and 14-24, and 26-36 are dependent upon Claims 1, 13, and 25, respectively, and are allowable. Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. 102(e).

III. CONCLUSIONS & MISCELLANEOUS

For the reasons set forth above, Applicant respectfully submits that all pending claims are patentable over the art of record, including the art cited but not applied. Accordingly, allowance of all claims is hereby respectfully solicited.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: January 6, 2005

Kirk D. Wong
Reg. No. 43,284

1600 Willow Street
San Jose, California 95125-5106
Telephone No.: (408) 414-1080 ext. 214
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on January 6, 2005 by